DAIDS
Bethesda, MD USA

POLICY
Draft Use of Electronic Information Systems in Clinical Research

Approval Date No.:
Effective Date:

Please submit comments to the **ProPEP Comment Coordinator** by **NOVEMBER 1, 2017**. Please include the following information: the name of the document, line number(s) and/or section number that corresponds. **Comments will only be accepted in the specified format.**

1.0 PURPOSE

The purpose of this policy is to describe the requirements for using electronic information systems to create, manage, and store electronic records in National Institute of Allergy and Infectious Diseases (NIAID), Division of Acquired Immunodeficiency Syndrome (DAIDS) supported and/or sponsored clinical research.

2.0 SCOPE

This policy applies to all NIAID (DAIDS) supported and/or sponsored clinical research.

3.0 BACKGROUND

The use of electronic informed consent, signatures, and source data capture in clinical research has become more common as investigators try to eliminate problems such as duplication of data and transcription errors, and promote such activities as real-time access for data to review. Regardless of what type of system (e.g., paper, electronic, or hybrid) is used by the clinical site to record source data, the requirements for source data and source documents are the same (e.g., source data by be attributable, legible, contemporaneous, original, and accurate). This policy describes the minimal requirements that information systems must meet for collecting, storing, transmitting, and securing private research data in an electronic format for NIAID (DAIDS) supported and/or sponsored clinical research. This policy is directed to ensure that data and applied systems have adequate protections in place to maintain confidentiality and integrity, while ensuring that such data is easily retrievable. The FDA regulations at 21 CFR Part 11 provide the technical requirements upon which this policy is based.

4.0 DEFINITIONS

For additional definitions, see DAIDS glossary.

Audit Trail: A process that captures details such as additions, deletions, user information, or alterations of data in an electronic record without obscuring the original record. An audit trail facilitates the reconstruction of the course of such

details relating to the electronic record. (FDA)

Data Originators: The original source of data. Each data element is associated with an origination type that identifies the source of its capture in the eCRF. This could be a person, a computer system, a device, or an instrument that is authorized to enter, change, or transmit data elements into the eCRF (also sometimes known as an author). Examples of data originators include:

- Clinical investigators and study staff
- Participants or their legally authorized representative
- Ancillary services representatives or other consultants such as radiologists, neurologists, etc.
- Devices such as electrocardiography (ECG) or blood pressure machines
- Electronic Health Records (EHRs)
- Automated laboratory reporting system (FDA)

Data Element: The smallest unit of observation captured for a participant in a clinical investigation. Examples of data elements include race, white blood cell count, pain severity measurement, or other clinical observations made and documented during a study. Each data element is associated with an authorized data originator. (FDA)

Electronic Case Report Form (eCRF): An auditable electronic record of information that generally is reported to the sponsor on each trial participant, according to a clinical investigation protocol. The eCRF enables clinical research data to be systematically captured, reviewed, managed, stored, analyzed, and reported. An eCRF is an example of an electronic record. (FDA)

Electronic Informed Consent (eIC): A form of electronic systems and/or processes that may employ multiple electronic media (e.g., text, graphics, audio, video, podcasts and interactive Web sites, biological recognition devices, and card readers) to convey information related to the study and to obtain and document informed consent from the study participant. (FDA)

Electronic Record: Any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system. (FDA 21 CFR 11.3(b)(6))

Electronic Source Data: The research data when initially recorded in an electronic

format. (FDA)

Electronic Signature (e-Signature): A computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature. (FDA 21 CFR 11.3(b)(7))

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (NIST)

Validation of Computerized Systems: A process of establishing and documenting that the specified requirements of a computerized system can be consistently fulfilled from design until decommissioning of the system or transition to a new system. The approach to validation should be based on a risk assessment that takes into consideration the intended use of the system and the potential of the system to affect human subject protection and reliability of trial results. (ICH GCP E6)

5.0 RESPONSIBILITIES

DAIDS Network Data Management Centers (DMCs)

The Network *DMC* is responsible for:

- identifying the appropriate computerized system to be used to create, modify, maintain, archive, retrieve, or transmit data;
- ensuring the appropriate level of system validation and/or verification is applied to meet regulatory agency and DAIDS compliance requirements;
- ensuring appropriate training, certification and ongoing training for the management of the applied computerized systems;
- development and deployment of eCRFs that are auditable and FDA 21 CFR 11 compliant;
- ensure that any e-Signature system used in a DMC information system for clinical research is FDA 21 CFR 11.3(b)(7)) compliant;
- validation of the DMC information systems used in clinical research per ICH GCP E6;
- providing and controlling system access control for authorized personnel, including site investigators and staff, DAIDS monitors and auditors, and regulatory inspectors; and

- maintaining staff training records for all DMC system users;
- maintaining accurate logs of all authorized DMC data originators (individuals and devices that are designated to enter data into the electronic system);
- retaining electronic records in accordance with applicable U.S. regulations, applicable local regulations, and DAIDS Policy on Storage and Retention of Clinical Research Records; and
- deployment of information systems that meet all system requirements per this policy including access control, audit trails, record retention, validation, operational checks, authority checks, and device checks.

Clinical Research Protocol Team

The *clinical research protocol team* must provide sufficient information in the protocol documents to the Institutional Review Board/Ethics Committee (IRB/EC) on:

- the intended use of information systems, such as for eCRF or eIC, and which devices that will be used to record electronic source data;
- the data elements to be captured in pre-defined fields of any eCRF;
- site security, and information and data policies at the location where the research is being conducted;
- information on the eIC, consent process, and use of electronic signatures; and
- a description of the electronic data flow from collection to storage.

IRB/EC

The *IRB/EC* is responsible for:

- determining if the plans, processes, and policies proposed for electronic source data and information systems are sufficient to maintain data confidentiality, integrity, and data availability;
- determining if e-signatures used to document eIC are legally valid within the local jurisdiction where the research is being conducted, and if e-signatures may be used in lieu of handwritten signatures for the specific research project being reviewed.
- reviewing the eIC to determine if the method used to document informed consent is appropriate, and approving the eIC and any subsequent amendments to the eIC in accordance with the HHS regulatory requirements for informed consent and other applicable requirements, and ensuring the eIC contains all

applicable elements of informed consent (see 45 CFR 46.116 General requirements for informed consent).

Clinical Research Site (CRS) Leader

The *CRS leader* is responsible for:

- reviewing site procedures for maintaining the systems that ensure that data have adequate protections in place to maintain confidentiality and integrity and are in compliance with applicable regulations, laws, and policies, including DAIDS Policy Requirements for Data Management and Statistics for DAIDS Funded and/or Sponsored Clinical Trials;
- maintaining accurate logs of all authorized data originators (individuals and devices that are designated to enter data into the electronic system);
- maintaining staff system training records for all system users;
- reviewing and signing completed electronic records for each participant;
- retaining electronic and paper research records in accordance with applicable U.S. regulations and DAIDS Policy on Storage and Retention of Clinical Research Records;
- providing direct data access to research records and source data for authorized personnel, including DAIDS monitors and auditors, and regulatory inspectors; and
- developing and maintaining site procedures for using the information system, as described in the DAIDS Policy for Manual of Site Operations.

DAIDS

The *DAIDS Program Officer (PO)* is responsible for approving non-Network data management plans.

The *DAIDS Network PO* is responsible for approving the Network's data management plans.

6.0 POLICY

6.1 Computerized Information Systems and Devices Requirements

Computerized Information systems and data originator devices used in NIAID (DAIDS) supported and/or sponsored clinical research must have adequate controls in place to ensure confidence in reliability, quality, and integrity of the source data as related to risk to participants. The intended use of the system and the potential of the system to affect human subject protections and data integrity should be assessed for risk; the greater the risk associated with the information system or device, the more data security measures are needed.

The information system must have:

a. Access control, limiting system access to persons who have documented training and authorization with their own log-on and password. 21 CFR11.10(d)
b. An audit trail that records each entry made into an information system/device, the date and time data are entered, and to which research participant the data belongs; (the audit trail begins at the time the data are transmitted). Whenever any modification or correction to electronic data occurs the system must maintain an audit trail that records the date and time, as well as the name of the person who made the change. The system should have a field that allows the system user to include the reason for the change. Digital changes to the data must not obscure or delete the original entry, allowing others (including DAIDS monitors) to view both original and corrected electronic data. Alternatively, the corrected electronic record should be clearly labeled as such for future access. 21 CFR 11.10(e)
c. The ability to retain records in compliance with applicable regulations and to be available for inspection. 21 CFR11.10(c)
d. The capability to produce copies of electronic records. 21 CFR 11.10(b)
e. The ability to encode messages or information in such a way that only authorized parties can read it.

6.2 The performance requirements of the system must include:

a. Validation: The documented process of assuring that a computerized system does exactly what it is designed to do in a consistent and reproducible manner, consistent with FDA 21 CFR 11.10(a)
b. Operational Checks: Computer systems will have sufficient controls or operational system checks to ensure that users must follow required procedures. If it is necessary to create, delete, or modify records in a particular sequence, explain how operational system checks will ensure that the proper sequence of events is followed, consistent with FDA 21CFR11.10(f)
c. Authority Checks: The system will authorize users before allowing them to access or alter records, consistent with FDA21 CFR11.10(g). This may include different levels of security within the system. For example, a laboratory instrument may have only a few user groups (Standard User, Tester, Administrator, etc.), while a large electronic Data Management System may have dozens of user groups.
d. Device Checks: The ability of the system to perform an input check to ensure the source of the data being input is valid, consistent with FDA 21 CFR 11.10(h). In some cases, this means a monitor should be available such that someone entering data can see what they entered. This can also mean that data is restricted to particular input devices or sources. Data should not be entered into a regulated computer system without the owner knowing the source of the data. In other words, device has controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine.

6.3 System users (including system administrators) will:

a. Be trained before they are assigned tasks in the system, consistent with FDA 21 CFR 11.10(i). Documentation of system training will include of a listing of: trainee name(s), date of training, name of trainer, title of course, and primary contents covered in the training.
b. Follow the written policy and procedures that hold individuals accountable and responsible for actions initiated under their electronic signature/username and password, consistent with 21 CFR11.10(j). The policy prohibits individual users from allowing others to access the system

through their account/username/password and holds individual system users accountable and responsible for actions initiated under their electronic signature. Adherence to the policy will deter record and signature falsification.

6.4 System access is disabled if an individual user discontinues involvement during the study.

6.5 Electronic Informed Consent

The computerized system used in eIC must be secure with restricted access and have methods to protect the participant's confidentiality (e.g., encryption).

6.6 Electronic Source Data Capture System

The system that records electronic source data will include from where the data originated. This can be done through a password, log-on, identification code, or biometrics. The system must also maintain an audit trail, which tracks any changes made to the data, including the data and time the change was made, and the name of the person who made the change.

7.0 REFERENCES

FDA General Principles of Software Validation; Final Guidance for Industry and FDA Staff
Evidence Product Checklist For the FDA Document General Principles of Software Validation; Final Guidance for Industry and FDA Staff
FDA Guidance for Industry, Electronic Source Data in Clinical Investigations, 2013
FDA Guidance for Industry, Electronic Records: Electronic Signatures – Scope and Application, 2003
FDA Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices, 1999
FDA Use of Electronic Informed Consent in Clinical Investigations, Questions and Answers, 2015
ICH GCP E6 R2
NIST IR 7298 Revision 2, Glossary of Key Information Security Terms

8.0 INQUIRIES

Questions and comments regarding this policy may be directed to the OPCRO Policy Group

9.0 AVAILABILITY

This policy is available electronically on the Division of AIDS (DAIDS) Clinical Research Policies and Standard Procedures webpage.

10.0 APPENDICIES

None

11.0 APPROVAL